UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,573	10/18/2001	Jukka Alve	4208-4040	7887

27123 7590 08/03/2007
MORGAN & FINNEGAN, L.L.P.
3 WORLD FINANCIAL CENTER
NEW YORK, NY 10281-2101

EXAMINER	
JUNG, DAVID YIUK	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
08/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/982,573	ALVE ET AL.	
	Examiner	Art Unit	
	David Y. Jung	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *7-13,55-58 and 95-98* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *7-13,55-58 and 95-98* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 7-13, 55-58, 95-98 are presented.

CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-13, 55-58, 95-98 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hahn (http://www.w3.org/2000/12/drm-ws/pp/versaware-hahn.html) and Menezes (cited by Applicant, MENEZES, A. et al. "Ch. 13 Key Management Techniques", CRC Press, Inc., 1997, XP-02423026, pp. 548-572.) and Poorvi (http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html).

Regarding claim 7, Hahn teaches "A method of moving protected content within an authorized [ ] comprising: transmitting encrypted content and a voucher associated with said encrypted content from a first device in the authorized [ ] to a second device in the authorized domain (Hahn section 2.3.2.1 Rights Expression, i.e., vouchers, section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); the voucher including an encrypted content key (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations) and [ ];

at the first device rendering any vouchers associated with said encrypted content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 8: The method of claim 7 further comprising:

encrypting the entire voucher.

Such encryption is well known in the art for the completeness of security (entire voucher being encrypted would be more complete).

Claim 9, 10

9. The method of claim 7 further comprising:

receiving said encrypted content and the voucher associated with that content in a second device in the authorized domain.

10. The method of claim 9 comprising:

decrypting the encrypted content key at the second device; and

using the decrypted content key to decrypt the encrypted content.

. Such use of second device is well known in the art of DRM for the motivation of transfer of content. For example, peer-to-peer spread of content would be possible and yet the payment for content would also be guaranteed -- so as to protect data. The new user at a second device would get the encrypted content but would need to also separately get the key in order to decrypt the content.

Claim 11: Hahn teaches A method for moving protected content from a first device in one authorized [ ] to a target device in a different authorized [ ] comprising:

checking a voucher associated with a piece of content;

the voucher including an encryptyed content key, [ ], a [ ] traversal flag(Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

if [ ] allows moving, decrypting the encrypted content key with a device key (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); and

encrypting the decrypted content key with the public key of the target device;

replacing the original encrypted content key with the re-encrypted content key in the voucher (Hahn section 2.3.2.3 Rights Management, i.e., voucher

management and content key operations);

transmitting encrypted content and the amended voucher to the target device (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); and

at the first device rendering any vouchers associated with the content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 12: The method of claim 11 where the device key used to decrypt the encrypted content key is a private key of the first device.

Such use of private key is well known for the motivation of decryption in digital rights management.

Claim 13: The method of claim 11 further comprising:

decrypting the voucher received at the target device using a private key associated with the target device's public key;

decrypting the encrypted content using the decrypted content key from the voucher.

Such use of public key algorithms is well known for the motivation of asymmetric encryption and thereby data protection.

Claim 55: Hahn teaches An article of manufacture comprising:

a computer readable medium comprising instructions for: transmitting encrypted content and a voucher associated with said encrypted content from a first device in an authorized [ ] to a second device in the authorized [ ] (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

the voucher including an encrypted content key and [ ] (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

at the first device rendering any vouchers associated with said encrypted content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 56: The computer readable medium of claim 55 further comprising instructions for: encrypting the entire voucher.

Such encryption is well known in the art for the completeness of security (entire voucher being encrypted would be more complete).

Claim 57: Hahn teaches An article of manufacture comprising:

a computer readable medium comprising instructions for: on a first device checking a voucher associated with a piece of content (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

the voucher including an encrypted content key, [ ] and a [ ] traversal flag (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

if [ ] allows moving, decrypting the encrypted content key with a device key (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); and

encrypting the decrypted content key with the public key of a target device (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

replacing the original encrypted content key with the re-encrypted content key in the voucher (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

transmitting encrypted content and the amended voucher to the target device (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); and

rendering any remaining vouchers associated with the content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 58: The article of manufacture of claim 57 where the device key used to decrypt the encrypted content key is a private key of the first device.

Such use of private key is well known for the motivation of decryption (in both private key algorithms and public key algorithms) in digital rights management.

Claim 95: Hahn teaches An apparatus capable of moving protected content within an authorized [ ] comprising:

means for transmitting encrypted content and a voucher associated with said encrypted content from said apparatus to a second device in the authorized [ ] (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

the voucher including an encrypted content key and [ ] (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

means for rendering any vouchers associated with said encrypted content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 96: The apparatus of claim 95 further comprising:

means for encrypting the entire voucher.

Such encryption is well known in the art for the completeness of security (entire voucher being encrypted would be more complete).

Claim 97: Hahn teaches An apparatus capable of moving protected content to a target device in a different authorized domain comprising: means for checking a voucher associated with a piece of content (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

the voucher including an encrypted content key, a usage state record and a domain traversal flag (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

means for decrypting the encrypted content key with a device key (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

means for encrypting the decrypted content key with the public key of the target device (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

means for replacing the original encrypted content key with the re-encrypted content key (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations);

means for transmitting encrypted content and the amended voucher to the target device (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations); and

means for rendering any vouchers associated with the content unusable (Hahn section 2.3.2.3 Rights Management, i.e., voucher management and content key operations).

These passages of Hahn do not teach "domain" in the sense of the claim.

Menezes teaches "domain (chapter 13, section 13.5.1 Key separation and constraints on key usage, i.e., key separation" for the motivation of security.

These passages of these references do not teach "usage state record" in the sense of the claim.

Poorvi teaches "usage state record (section 4 Example outcome of the workshop, especially section 4.1, i.e., usage tracking" for the motivation of digital rights management.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Hahn and Menezes for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claim 98: The apparatus claim 97 where the device key used to decrypt the encrypted content key is a private key of the apparatus.

Such use of private key is well known for the motivation of decryption (in both private key algorithms and public key algorithms) in digital rights management.

Conclusion

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Kambiz Zand whose telephone number is (272) 272-3811.

David Jung

Patent Examiner

8/1/07